Joanne

SUMMARY

OF

SECURITY REQUIREMENTS FOR

CONTRACTOR AUTOMATED INFORMATION SYSTEMS

PROCESSING SENSITIVE COMPARTMENTED INFORMATION

SCIREQ-004

EXECUTIVE SUMMARY

The Customer's Sensitive Compartmented Information (SCI) must be protected in accordance with applicable intelligence community directives. This Sensitive Compartmented Information Requirements Document (SCIREQ-004) interprets and enhances, for the Customer, the policies contained in those directives.

SCIREQ-004 establishes security requirements for protecting the Customer's SCI processed on Contractor-operated mainframe computers and associated peripheral equipment, personal computers, office automation systems, and hand-held calculators, collectively termed Automated Information Systems (AIS). SCIREQ-004 also establishes security requirements for protecting the Customer's SCI processed by networks.

Prior to using an AIS, or network, for processing Customer data, the Contractor must provide the required AIS security program documentation to the Customer for approval (See SCIREQ-004).

The Customer will approve the security controls for each Contractor AIS or network processing SCI, in close coordination with the Contracting Officer's Security Representative (COSR), the Contracting Officer's Technical Representative (COTR), the Customer's COMSEC Representative, and the Contractor's Automated Information System Security Representative (AISSR).

While some small or special-purpose AIS's, by design, may not be able to meet the requirements established in SCIREQ-004, it may be necessary to impose additional security requirements on other AIS's. Resolution of these case-by-case situations will be determined by the assigned Customer ISSO, in close coordination with the COTR, COSR, and Contractor AISSR.

The basic document is divided into eight chapters, supporting appendices, and an attachment. The first four chapters describe Contractor and Customer responsibilities, audits, certifications, modes of operation, AIS security standards, facility construction standards, emission control standards, and network security standards.

The latter four chapters cover personnel access, system operational requirements, system maintenance, configuration management, media control, and documentation and training requirements. The appendices and the attachment provide guidance designed to assist the Contractor in conforming to the requirements discussed in the document's basic eight chapters.

The attached Summary provides a quick reference, by chapter, of the AIS security requirements specified in SCIREQ-004.

CHAPTER 1

INTRODUCTION

CHAPTER 1 - INTRODUCTION

Purpose

- Specify Customer security policy and requirements for the selection, installation, operation, maintenance, and configuration management of automated information systems (AIS).

- Provide guidance in the preparation of the required AIS Security Program Plan.

Scope

- Applies to all Contractors processing sensitive compartmented information (SCI).

- Does not apply to AIS's used exclusively for telecommunications services.

Responsibilities

Contractor

Designate an Automated Information System Security Representative (AISSR). The AISSR will:

- Establish and maintain a formal AIS security program.

- Prepare and submit for approval, an AIS Security Program Plan. See Chapter 8 for guidance.

- Prepare, for AIS's designed to process in the COMPARTMENTED MODE, a Certification Test Plan. See ~~Chapter 8 for guidance~~.

- Maintain all AIS related system, operation, program, and user documentation in the current revision.

- Maintain a central repository for all AIS security program request actions, plans, and Customer approvals.

- Maintain a Special Program Documentation Control Center to account for all SCI documentation and magnetic media.

° Coordinate all AIS-related security actions with the assigned Customer ISSO.

° Establish and maintain a formal system for the assignment, distribution, and control of system logon passwords.

° Provide for the execution, as required, of appropriate memorandums of agreement.

Customer

The Customer assigned Information Systems Security Officer (ISSO) will:

° Approve the security controls and safeguards for each AIS processing SCI.

° Evaluate and issue ISSD's written approval of each AIS Security Program Plan for which responsible.

° Evaluate and issue ISSD's written approval of each AIS Certification Test Plan for which responsible.

° Coordinate all Contractor AIS security requests.

° Coordinate Customer directives applicable to the handling, storage, transmission, and destruction of SCI.

° Periodically visit, audit and, as required, conduct certification tests of the assigned AIS's.

The Contracting Officer's Security Representative (COSR) will:

° Coordinate Customer approvals for physical, COMSEC, and AIS security.

° Determine the handling, storage, transmission, and disposition of magnetic media.

° Coordinate all security deficiencies requiring an Engineering Change Proposal and notify ISSD of any formal proposals requiring a contractual change.

The Customer's Communications Security Officer (COMSEC) will:

° Determine the complete spectrum of COMSEC requirements for each AIS processing SCI.

° Evaluate and issue COMSEC's written approval of all AIS Security Program Plans for which responsible.

° Coordinate Customer directives requiring Customer approval with the assigned ISSO, Contractor AISSR, and the COSR.

° Periodically visit and audit assigned AIS's.

Audits and Certifications

AIS Security Audit

° Verifies that the hardware and software listed in the approved AIS Security Program Plan are in place and being used.

° Normally scheduled every 24 months for each major AIS processing SCI

AIS Security Certification Test

° Certification test and evaluation are prerequisites for Customer issuance of a formal written Processing Approval for a Contractor's AIS to process in the Customer-defined COMPARTMENTED MODE.

CHAPTER 2

SYSTEM SECURITY

CHAPTER 2 - SYSTEM SECURITY

Modes of Operation - Definitions

Dedicated Mode

Processing one or more SCI compartments, usually in support of a single project.

Each user with access to the AIS has:

° A valid DCID 1/14-based personnel clearance.

° A DCID 1/19 access approval for all SCI stored in or processed by the AIS

° A valid need-to-know know for all SCI contained within the AIS

System High Mode

Processing one or more SCI compartments usually in support of two or more projects.

Each user with access to the AIS has:

° A valid DCID 1/14-based personnel clearance.

° A DCID 1/19 access approval for all SCI stored in or processed by the AIS

° A valid need-to-know know for some or all SCI contained within the AIS

Compartmented Mode

Processing two or more SCI compartments in support of two or more projects.

Each user with access to the AIS has:

° A valid DCID 1/14-based personnel clearance.

° A DCID 1/19 access approval for that SCI to which the user is to have access

° A valid need-to-know know for that SCI to which the user is to have access

Security Standards for AIS's

Dedicated Mode

° Be located in an approved SCIF

° Enforce a system logon for

°° Individuals authorized to boot the AIS

°° All system users

° Prohibit any applications program from seizing control, or writing data into, space assigned to the operating system

° Rigorously control all system hardware and software

° Enforce, following execution of system recovery procedures, the logoff of all system users prior to allowing a system logon.

° Provide for one class of machine instructions reserved for exclusive use of the operating system.

° Control and protect the unauthorized modification of the operating system and applications programs.

° Provide an audit trail capability that, at a minimum, accurately reflects both USERID activity and unauthorized attempts to access the AIS

° Provide for the proper security classification level marking of all system generated human readable output.

System High Mode

° Meet all security standards for Dedicated Mode, and

° Limit the use of system privileges to those persons having an established need-to-know.

° Define and control access between system users and named objects.

° Provide an audit trail capability that records, in addition to requirements specified for the Dedicated Mode, the use of identification mechanisms, introduction of objects into a users address space, and the deletion of objects.

Compartmented Mode

° Meet all security standards for Dedicated Mode and System High Mode, and

° Support a trusted communications path between itself and each system user for initial logon verification.

° Assure restriction of user's access to those portions of the SCI processed by the AIS for which the user is authorized.

° Enforce compartmentation and provide rigorous need-to-know controls with each compartment.

° Enforce, under system control, a system-generated security classification banner at the top and bottom of each physical page of output.

° Enforce an upgrade/downgrade principle where

°° All sessions have a system maintained classification

°° No data is read which is classified higher than the session

°° No data is written unless its classification is equal to the session's classification.

° Prevent residue, from previous use of the object, from being available in central memory.

° Provide an audit trail capability that records, in addition to those requirements specified for the Dedicated Mode and System High Mode, the routing of all system jobs and output.

MODES OF OPERATION SUMMARY MATRIX

Operating Mode	Lowest level of "USER" Clearance	Formal Access Approval	Need to Know	Class of Trust*
DEDICATED MODE	DCID 1/14 adjudicated & approved by applicable customer	All data on system	All data on system	C1
SYSTEM HIGH MODE			Only some data on system	C2
COMPARTMENTED MODE		Only some data on system		B1**

* Class of Trust required. Prior to the year 2000, these requirements may be achieved with functional equivalents. (Reference DOD 5200.28-STD , "Department of Defense Trusted Computer System Evaluation Criteria.")

** Currently B1, plus requirement to ptovide a trusted communications path for initial logon and verification, a B2 requirement.

CHAPTER 3

FACILITY SECURITY

CHAPTER 3 - FACILITY SECURITY

Computing Facility

Operator consoles and control terminals must be located in the same room as the host computer.

Emission Security (TEMPEST)

TEMPEST Security Factors

Includes the TEMPEST profile of the hardware, the type and quality of the TEMPEST countermeasures incorporated in the facility, and the size for the controlled space surrounding the installation.

TEMPEST Certification Requirements

Because these requirements are classified, please refer to SCIREQ-004.

Interface Circuit Restrictions

- Interconnections between AIS equipment and mainframes require prior approval of the COSR

- Classified AIS's may be interfaced with a classified mainframe computer in the same building.

- Prior Customer approval required to run connections through an unclassified area.

- Connection to a mainframe computer that is exterior to the approved facility must be encrypted.

- An AIS used exclusively for unclassified processing may not be interfaced with or connected to an unclassified mainframe outside the approved facility without approval of the COSR.

- Modems used to connect unclassified AIS's are strongly discouraged.

- Dial-up modems are prohibited

CHAPTER 4

NETWORK SECURITY

CHAPTER 4 - NETWORK SECURITY

Network Responsibilities

Contractor

Designate an individual to act as the Contractor's Network Security Representative (NSR). The NSR will:

° Establish and maintain a formal Network Security Program

° Prepare, and submit for approval, a Network Security Program Plan for each proposed network.

° Develop, for each network designed to operate in the Compartmented Mode, a Network Certification Test Plan which must have prior approval of both the COSR and ISSD.

° Coordinate all network-related security actions with the assigned Customer ISSO.

Customer

The Customer assigned ISSO will:

° Approve the security controls and safeguards for the proposed network

° Coordinate all network security actions requiring Customer approval.

The Customer assigned COMSEC representative will:

° Review and approve the communications security aspects of the proposed network.

Network Security Standards

Modes of Operation for Networks

Dedicated Mode

A network is operating in the Dedicated Mode when:

° Each user of the network has a DCID 1/14 clearance

° Each user has all the appropriate formal access approvals

° Each user has need-to-know for all data present in the network.

° The network is accredited to operate for a specific set of SCI compartments.

° Each AIS on the network is separately accredited to operate in the Dedicated Mode.

System High Mode

A network is operating in the System High Mode when:

° Each user of the network has a DCID 1/14 clearance

° Each user has all the appropriate formal access approvals but not necessarily the need-to-know for all information in the network.

° The network is accredited to operate for a specific set of SCI compartments.

° Each AIS on the network is separately accredited to operate in the System High Mode.

° Each AIS and the network are accredited for the same security level.

Compartmented Mode

A network is operating in the Compartmented Mode when:

° Each user of the network has a DCID 1/14 clearance but not necessarily the formal access approvals for all SCI in the network, nor need-to-know for all SCI in the network.

- The network is accredited for handling SCI of a common classification, but of multiple compartments.

- Each AIS on the network is separately accredited to operate in the Compartmented Mode.

- Each AIS on the network has an accreditation range that includes one or more of the approved SCI compartments of the network's accreditation range.

Network Hosts

Network hosts shall:

- Identify and verify each network user and be responsible for network access and all auditing.

- Transfer sensitivity (SCI) labels for all SCI exchanged with other network hosts.

- Protect user/host identifiers and sensitivity labels.

Network Subsystems

Network-specific software shall perform only network-specific functions

The network-specific audit trail shall, at a minimum, provide for the weekly review of:

- Each connection and its principal parameters

- Starting and ending times of each connection

- Security-relevant exceptional conditions detected during a connection

- Information needed to associate network-specific audit trail records with the corresponding host audit trail records.

Network Standards

Dedicated Mode

° Each network user must have DCID 1/14 clearance, formal access approvals and need-to-know for all SCI processed.

° The network must be accredited to operate in the Dedicated Mode.

° Each network host must be separately accredited to operate in the Dedicated Mode and to participate in the network at the specific security level of the network.

System High Mode

° Each network user must have DCID 1/14 clearance, formal access approvals for all compartments processed, but not necessarily be approved need-to-know for all SCI processed.

° The network must be accredited to operate in the System High Mode at a specific SCI security level.

° Each network host must be separately accredited to operate in the Dedicated Mode or System High Mode and to participate in the network at the specific security level of the network.

Compartmented Mode

° Each network user must have DCID 1/14 clearance, formal access approval for at least one of the SCI compartments processed, but not necessarily be approved need-to-know for all SCI processed.

° Each terminal shall be assigned to a home host

° Hosts participating in Compartmented Mode processing shall:

°° Identify the security SCI classification level of each participating terminal

°° Determine that the identified security SCI classification level is appropriate.

° Each host participating in a Compartmented Mode network must be capable of asserting the correct network SCI security level for output.

° Each network host shall transfer sensitivity (SCI) labels for all information exchanged with other network hosts

° Each host initiating a network connection session shall be identified to the other host once each connection.

° Each network user shall be identified to each host each time an access connection is initiated.

CHAPTER 5

ACCESS AND OPERATION

CHAPTER 5 - ACCESS AND OPERATION

Clearance and Access

Personnel Access

° All personnel requiring unescorted access to an AIS must be DCID 1/14 cleared and have formal access approval for all data processed.

° Access to system console terminal must be limited to designated operations personnel

° The need-to-know criteria will be enforced.

° Access to vaults will be limited to personnel who are DCID 1/14 cleared and have formal access approval for all data stored.

° Access to areas used to store the Customer's SCI will be limited to the individuals assigned media control duties.

° Approval for visits to an AIS must be requested in advance on a case-by-case basis and approved by the AISSR, at the direction of the COSR.

AIS Access Control

° AIS access must be limited to the custodian, alternate custodian, and users who have a valid need-to-know.

° Access to an AIS terminal must be limited to those users who possess a DCID 1/14 clearance, a formal access approval for the highest security classification level and SCI control channel(s) processed.

° Any AIS terminal authorized for unclassified data only shall be clearly labeled as such and an authorized access list will be posted at the terminal.

System Passwords

User access to an AIS used to process SCI must be controlled through the use of a unique system logon password.

The AISSR is responsible for the System Logon Password Management System.

Password Requirements

° System logon passwords will be randomly selected pronounceable words between six and eight characters in length, and will not all be the same length.

° System logon passwords must be verified by the system each time the user attempts to access the system.

° The number of system logon password entry failures will be limited to three.

° System logon passwords must not be displayed at any terminal or printed at any printer.

° System logon passwords will not be shared by system users.

° The assigned USERID will be deleted from the system when a system user leaves the Program/Project or following a suspected or known compromise.

° System logon passwords will be treated as SECRET insofar as issuance, handling, and storage.

° System logon passwords will be changed every 6 months, or sooner if required by the ISSO.

System Preparation

° Computing facility and remote terminal areas must be secured.

° Conductive devices not related to the processing must meet Red/Black separation requirements.

° Input/output devices, remote terminals, and direct access devices not to be used during processing operations must be disconnected.

° The system software must ensure that no illegal devices or communications links are activated.

° Demountable magnetic media not to be used during processing will be placed in secure storage.

° Non-demountable magnetic media to be used exclusively for processing Customer SCI may be connected to the system provided their use has been approved by the ISSO.

° The CPU memory must be sanitized.

° A separate copy of the operating system will be used to initialize the system.

Data Processing

° An adequate number of personnel will be present during processing operations.

° Remote terminals and printers will be individually designated for system use.

° Alpha-numeric slave printers are prohibited.

° The use of special purpose plotter type printers must be approved, in advance, by the ISSO.

° Data files must contain only data records related to processing the Customer's SCI

° Audit trail capability must be used to record

°° Unauthorized attempts to access the system

°° Authorized system users who attempt to access an unauthorized program or date file.

°° USERID; User Program/office assignment; terminal ID and location; Date; Start/stop time of activity; and type of activity.

° Unattended batch processing must have open shelf storage approval

° Should a security-related abnormal processing operation occur, processing must be stopped until the AISSR can determine the appropriate action.

° Following a security-related abnormal system operation, a dedicated copy of the operating system will be used for system reinitialization.

° Abnormal system operations, security violations and infractions will be reported to the COSR and the ISSO.

° Emergency situations must be reported to the COSR and the ISSO.

° System users are responsible for system safety and security.

Mode Termination

° The CPU memory must be sanitized.

° All connected peripheral devices must be powered down.

° Demountable magnetic media must be demounted and placed in approved storage.

° All printer ribbons must be removed and secured.

° A test pattern must be printed three (3) times to clear any latent image from all laser printers.

° Any fixed storage media device required for data storage or for permanent storage of the operating system and dedicated to the Program/Project processing period being terminated, must be physically disconnected from the system.

° The card path of each reader/punch will be operated for 3 card cycles.

° Any system management capability used for project accounting will be dumped to a demountable storage media.

° System generated ouput, hardcopy output, and magnetic media will be handled at the highest security classification level until certified at a lower level.

° Classified waste will be destroyed.

° Audit trail records will be reviewed on a weekly basis.

CHAPTER 6

HARDWARE AND SOFTWARE CONTROL

CHAPTER 6 - HARDWARE AND SOFTWARE CONTROL

Maintenance Policy

° Vendor maintenance personnel shall possess a valid security clearance.

° Uncleared vendor maintenance personnel must be monitored at all times by an individual who:

°° Is approved by the AISSR

°° Is technically knowledgeable of the equipment to be repaired.

°° Possesses a valid security clearance and access approvals for the security classification level and SCI control channels processed by the equipment.

° When systems containing integral non-removable disks require maintenance by uncleared vendor personnel, the vendor personnel must be denied visual access to any SCI data.

° Any deviation from these requirements must be approved by the ISSO.

° All maintenance and diagnostics shall be performed in the SCI facility.

° Any component released from secure control for any reason may not be returned to the special program area.

Maintenance Software and Remote Diagnostic Links

° A separate, dedicated-for-maintenance, copy of the operating system will be used for all unclassified maintenance.

° Procedures for an AIS using a non-removable direct access device on which the operating system is resident will be separately approved by the Customer on a case-by-case basis.

° Vendor-supplied software/firmware used for maintenance or diagnostic must be maintained within the secure facility.

° The Customer discourages the use of remote diagnostic links. The use of a remote diagnostic links must be approved by the ISSO before implementation.

Components

° Malfunctioning components shall be either repaired within the SCIF or replaced using a factory-fresh component.

° Components with all volatile memory may be released from the secure area only after preparation of an "Equipment/Media Sanitization and Release Record."

° Components with nonvolatile memory should, in general, be destroyed. If they must be released, they may be released only after complete sanitization, preparation of an "Equipment/Media Sanitization and Release Record" and written approval by both the AISSR and the ISSO.

Personal Computer Management

Policy for Stand-Alone PC's

° Contractor must submit a PC Security Plan for approval prior to installing any PC.

° PC use in a special program area is restricted as follows:

°° All PC's must be registered with and approved by the ISSO

°° All PC's must be either Government Furnished, Contractor-owned, or Contractor-leased.

°° No personally-owned PC's are allowed in special program areas.

°° Dial-up modems are not permitted to be connected to any stand-alone PC.

°° PC's designated for unclassified use must not be used for any classified processing.

° Each stand-alone PC designated for unclassified processing must be labeled "UNCLASSIFIED WORK AND MEDIA ONLY".

PC Registration and Approval

° A "Personal Computer Registration Sheet" will be prepared with a volatile memory certification attached, as required.

° Completed PC registration sheets will be submitted by the AISSR to the ISSO via the COSR.

° After registration, PC hardware and location shall not be changed without prior approval by the ISSO

PC Control

° Each PC will be assigned to a Custodian who is responsible for the following:

°° Monitor assigned stand-alone PC's on a daily basis

°° Maintain, and periodically update all "Authorized PC User Lists".

°° Assure that users of assigned unclassified stand-alone PC's are aware of the restrictions for using such PC's.

Hand-Held Calculator Management

Policy

° Applies to both company-owned and personally-owned hand-held calculators.

° Hand-held calculators that contain strictly volatile memory do not require registration.

° Hand-held calculators containing nonvolatile memory must be registered with and approved by the Customer.

° Hand-held calculators will be controlled and stored commensurate with the highest security classification level and SCI control channel of the data.

° The AISSR must establish the policy for removing hand-held calculators from special program areas, but all calculators must be sanitized before being removed from the special program area.

Configuration Management

CM Program Objectives

° Program should include an approach for specifying, documenting, controlling, and maintaining the visibility and accountability of all hardware, software, interfaces, operating procedures, and installation structures.

° The CM Program should include:

°° Organizational relationship of CM to total project management

°° A method for identifying the trusted baseline of each AIS

°° The methods, procedures, and policies for controlling the AIS trusted baseline.

°° A configuration accounting system.

°° Milestones for implementation of the CM Program.

Configuration Control Board

° Should consist of the AISSR, management and technical representatives and clerical personnel, as needed.

Configuration Identification

° The Customer will review and approve all changes to the defined trusted baseline.

Configuration Accountability

° CM Program should be used to record approved configuration change request documents and the implementation status of all approved changes.

Configuration Verification

° CM Program should be capable of verifying that the operation of each AIS is in accordance with approved documentation.

AIS Hardware and Software Identification

° All AIS hardware and software should be identified with: Manufacturer, title or name, model number, part number, and serial number.

AIS Hardware and Software Change Control

° Temporary changes must be documented and approved by the AISSR. Evidence must be available that the AIS was returned to original state after temporary change.

° Permanent changes must be covered by documentation approved by the Customer.

Documentation Change Control

° The AIS must be installed and operated according to the latest applicable and approved documentation.

Audits

° Formal audits may be conducted by the Customer to ensure that the CM Program, if one exists, is in conformance with the Customer's objectives.

CHAPTER 7

MEDIA CONTROL

CHAPTER 7 - MEDIA CONTROL

Printed Media Control

Marking

° Classified printed output must be marked with the security classification level and associated markings at the top and bottom of each physical page.

° For working material, the words "Working Material - Destroy by: (Date)" must be attached to the from of the material in addition to the Security classification level and SCI control channel information.

° Unclassified printed output must be marked "UNCLASSIFIED".

Control

° A Document Control Number must be assigned and placed on the front of each controlled SCI document.

Secret Working Material

° SECRET SCI working material, which will be retained less than 90 days, does not require a Document Control Number.

° SECRET SCI working material retained longer than 90 days must have a Document Control Number placed on the material's pre-printed title page.

Unclassified Documents

° Hardcopy documents must be handled at the highest security classification level of the processing period until reviewed and certified at a different security classification level, including unclassified.

Storage

° All classified printed material must be stored in classified material containers per Customer directives.

Magnetic Media Control

Policy

- All magnetic media acquired for use on either classified or unclassified systems must be treated and controlled as classified.

- The use of direct access storage devices, with fixed disks, for the storage or processing of SCI must be approved, in writing, by the Customer.

- Each direct access device must have affixed to it a sign or label indicating the highest security classification level and SCI control channel(s) of the information ever stored on the media.

- The area which houses fixed disk direct access storage devices must be approved by the Customer for Open Storage.

Accountability

- A central accountability and annual inventory system for all unclassified and classified magnetic media will be established and maintained.

Registration

- All magnetic media must be assigned a "Magnetic Media Control Number", registered, and placed under control of the Special Program Document Control Center.

Marking

- An external label must be affixed to demountable magnetic storage media to clearly indicate the highest security classification level, including Unclassified, and SCI control channel(s) of the information ever recorded on the media.

Software

- Magnetic-media-resident software to be obtained from external sources for use in diagnostics or maintenance must be acquired from authorized sources only and approved by the AISSR.

Removal of Unclassified Magnetic Media

- Written justification must be provided to the AISSR requesting removal of the media and giving a description of the contents.

- Prior to removal, a printout of the media contents must be generated and verified.

- The verification procedure entails a complete hardcopy or softcopy dump and review of the media contents and the completion of an "Equipment/Media Sanitization and Release Record."

- Removal of magnetic media containing program software is further restricted and may be permitted on a case-by-case basis but only prior approval of ISSO.

Removal of Classified Media

- Movement of demountable media on which SCI is recorded must be approved by the AISSR.

- Written justification must be provided to the AISSR requesting removal of the media and giving a description of the contents.

- The data must be written onto new factory-fresh media.

- Only the factory-fresh media may be released.

- The requester must complete an "Equipment/Media Sanitization and Release Record

Packaging and Transportation

- Classified media must be transported by security personnel authorized by the COSR.

Magnetic Media Storage

- Demountable magnetic media containing SCI must be stored in a Customer-approved security container.

- When a system is approved for "Periods Processing" and the system uses direct access storage devices with fixed disks, the storage device must be physically and logically disconnected when the system is not being used to process the Customer's SCI.

Other Media Control

Card decks and punched paper tape shall be marked to indicate the highest security classification level, including unclassified, and SCI control channel(s) of the information contained on the deck.

Used printer ribbons must be stored in approved containers and must be destroyed under the guidance of the AISSR.

Printer platens must be inspected and either cleaned, if required, or removed and stored in approved classified containers.

Sanitization and Destruction

Policy

° SCI storage media may not be released from classified control, even though sanitized, without written approval of the COSR, the data owner, and the ISSO.

° All records of media sanitization will be retained for a period of at least two (2) years, except TOP SECRET SCI media sanitization records will be retained for a period of three (3) years.

° Only approved degaussing equipment will be used for media containing classified information.

Standards

° The overwrite method is to write over every addressable location first with one pattern, usually binary "one" digits, and then with the complementary pattern, usually binary "zero" digits for a total of three cycles.

Risk Considerations

° Risk factors such as destination of released media, effects of heat and age, mechanical storage device equipment failure, storage device segments not receptive to overwrite, inter-record gap problems, and degaussing equipment failure will be considered by the data owner before approving media release.

Sanitization Procedures

° Type 1 Magnetic Tapes (Magnetic tapes with coercivity factors not exceeding 325 oersted)

° Type 2 Magnetic Tapes (Magnetic tapes with coercivity factors exceeding 325 oersted)

° Diskettes, Magnetic Cassettes, and Magnetic Cards

° Operable Digital Equipment Corporation (DEC) RM03, RM05, RP06, RP07, (Fixed), RA60, RA80 (Fixed), and RA81 (Fixed) Disks

° Operable IBM 3350, 3370, and 3380 Hard Disks

° Operable Disk Storage Devices (Including Winchester Technology Disks and Magnetic Drums)

° Inoperable Disk Storage Devices (Not including Winchester Technology Disks)

° Inoperable Winchester Technology Disks

° System Internal Memory Sanitization

° Sanitization of Hand-held Calculators

Destruction Procedures

° Disks, disk packs, diskettes, magnetic tapes, magnetic cassettes, magnetic cards, and magnetic strips shall be sanitized prior to destruction and should be destroyed when they are no longer useful.

° Preferred destruction method is incineration

° Alternative method is disintegration using a SEM 1012 or SEM Model 22 with a screen size of 3/32 to 1/8 inch.

CHAPTER 8

DOCUMENTATION AND TRAINING

CHAPTER 8 - DOCUMENTATION AND TRAINING

AIS Security Program Plan

AIS Certification Test Plan Preparation

System Documentation

System User Training